refuses to execute the SF–312, the licensee or other facility shall deny the employee access to classified information and submit a report to the CSA. The SF–312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

(e) Initial Security Briefings. Before being granted access to classified information, an employee shall receive an initial security briefing that includes the following topics:

(1) A Threat Awareness Briefing.

(2) A Defensive Security Briefing.

(3) An overview of the security classification system.

(4) Employee reporting obligations and requirements.

(5) Security procedures and duties applicable to the employee's job.

(f) Refresher Briefings. The licensee or other facility shall conduct periodic refresher briefings for all cleared employees. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and by issuing written materials on a regular basis.

(g) Debriefings. Licensee and other facilities shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's access authorization is terminated, suspended, or revoked; and upon termination of the Facility Clearance.

(h) Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for three years after termination of the individual's access authorization.

[62 FR 17694, Apr. 11, 1997]

CONTROL OF INFORMATION

§ 95.35 Access to matter classified as National Security Information and Restricted Data.

(a) Except as the Commission may authorize, no person subject to the regulations in this part may receive or may permit any individual to have access to matter revealing Secret or Confidential National Security Information or Restricted Data unless the individual has:

(1)(i) A ''Q'' access authorization which permits access to matter classified as Secret and Confidential Restricted Data or Secret and Confidential National Security Information which includes intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information, or

(ii) An ''L'' access authorization which permits access to matter classified as Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section except that access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1984.

(2) An established ''need-to-know'' for the matter (See Definitions, §95.5).

(3) NRC-approved storage facilities if classified documents or material are to be transmitted to the individual.

(b) Matter classified as National Security Information or Restricted Data shall not be released by a licensee or other person subject to part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

(c) Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with §95.36.

[59 FR 48975, Sept. 23, 1994]

§ 95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.

(a) Based upon written disclosure authorization from the NRC Division of Security that an individual is an authorized representative of the International Atomic Energy Agency (IAEA) or other international organization and that the individual is authorized to make visits or inspections in

accordance with an established agreement with the United States Government, a licensee, certificate holder or other person subject to this part shall permit the individual (upon presentation of the credentials specified in §75.7 of this chapter and any other credentials identified in the disclosure authorization) to have access to matter which is classified National Security Information that is relevant to the conduct of a visit or inspection. A disclosure authorization under this section does not authorize a licensee, certificate holder, or other person subject to this part to provide access to Restricted Data.

(b) For purposes of this section, classified National Security Information is relevant to the conduct of a visit or inspection if—

(1) In the case of a visit, this information is needed to verify information according to §75.13 of this chapter; or

(2) In the case of an inspection, an inspector is entitled to have access to the information under §75.42 of this chapter.

(c) In accordance with the specific disclosure authorization provided by the Division of Security, licensees or other persons subject to this part are authorized to release (i.e., transfer possession of) copies of documents which contain classified National Security Information directly to IAEA inspectors and other representatives officially designated to request and receive classified National Security Information documents. These documents must be marked specifically for release to IAEA or other international organizations in accordance with instructions contained in the NRC's disclosure authorization letter. Licensees and other persons subject to this part may also forward these documents through the NRC to the international organization's headquarters in accordance with the NRC disclosure authorization. Licensees and other persons may not reproduce documents containing classified National Security Information except as provided in §95.43.

(d) Records regarding these visits and inspections must be maintained for five years beyond the date of the visit or inspection. These records must specifically identify each document which has been released to an authorized representative and indicate the date of the release. These records must also identify (in such detail as the Division of Security, by letter, may require) the categories of documents that the authorized representative has had access and the date of this access. A licensee or other person subject to this part shall also retain Division of Security disclosure authorizations for five years beyond the date of any visit or inspection when access to classified information was permitted.

(e) Licensees or other persons subject to this part shall take such measures as may be necessary to preclude access to classified matter by participants of other international agreements unless specifically provided for under the terms of a specific agreement.

[62 FR 17694, Apr. 11, 1997]

§95.37 Classification and preparation of documents.

(a) Classification. Classified information generated or possessed by a licensee or other person must be appropriately marked. Classified material which is not conducive to markings (e.g., equipment) may be exempt from this requirement. These exemptions are subject to the approval of the CSA on a case-by-case basis. If a person or facility generates or possesses information that is believed to be classified based on guidance provided by the NRC or by derivation from classified documents, but which no authorized classifier has determined to be classified, the information must be protected and marked with the appropriate classification markings pending review and signature of an NRC authorized classifier. This information shall be protected as classified information pending final determination.

(b) Classification consistent with content. Each document containing classified information shall be classified Secret or Confidential according to its content. NRC licensees or others subject to the requirements of 10 CFR Part 95 may not make original classification decisions.

(c) Markings required on face of documents.